

**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF PENNSYLVANIA**

IN RE Retreat Behavioral Health LLC

**Lead Case No.: 5:23-cv-00026-
MRP**

OPINION MEMORANDUM

Perez, J

March 7, 2024

Plaintiffs bring this putative data breach class action against behavioral and mental health service providers Retreat at Lancaster County PA LLC and Retreat Behavioral Health LLC (collectively “Defendants”). The case arises out of an unauthorized third-party ransomware attack of Defendants’ computer network wherein an unauthorized actor accessed personal information of Plaintiff class members. Presently before the Court is Defendants’ Motion to Dismiss (ECF No. 17), which argues that Plaintiffs have not demonstrated an injury-in-fact, an essential element for Article III standing in federal court.¹ The allegations in the complaint, accepted as true, fail to establish standing and therefore this Court lacks jurisdiction to hear the matter. For the reasons set forth below, Defendants motion to dismiss the case is granted.

I. BACKGROUND

Plaintiffs are individuals who received behavioral and mental health services from Defendants at their Lancaster facilities.² As part of their treatment, Plaintiffs provided Defendants with their social security numbers, dates of birth, and medical and treatment

¹ Defendant’s motion also argues, in the alternative, that the case should be dismissed for failure to state a claim. The Court need not address the merits in this matter because it lacks jurisdiction.

² Complaint (ECF No. 15) ¶¶ 1.

information, which was stored “unencrypted, in an Internet-accessible environment on Defendants’ network.”³ On July 1, 2022, Defendants experienced a ransomware attack during which unauthorized persons gained access to their computer systems and “may have accessed a data set” containing Plaintiffs’ personal identifiable information and protected health information (“PII/PHI”).⁴ Defendants immediately underwent a forensic investigation to determine the extent of the security breach, finding no evidence that Plaintiffs’ information was misused.⁵ At the conclusion of the investigation, Defendants notified states Attorneys General of the cyber-attack and sent notice of the breach to Plaintiffs.

Seeking damages and injunctive relief, Plaintiffs allege the following injuries resulting from the data breach: (1) “lost time, annoyance, interference, and inconvenience,” including time spent mitigating the risks of exposure and self-monitoring their accounts; (2) increased anxiety and concern for their loss of privacy; and (4) an increased risk of misuse, theft, and fraud. Plaintiffs do not allege that their information was ever used by the hackers or other third parties in any fashion. Their information was not published or sold on the Dark Web.

II. ARTICLE III STANDING

Standing restricts who can bring suit in federal court. This limitation ensures that federal judicial power extends only to resolving genuine disputes, rather than hypothetical disagreements, between parties. In the absence of standing, a plaintiff has no “case” or “controversy” empowering a district court to exercise jurisdiction. U.S. Const. art. III, § 2. To establish Article III standing, a plaintiff must establish: (1) she suffered a “concrete, particularized, and actual or imminent” injury-in-fact; (2) the injury “is fairly traceable to the

³ *Id.* at ¶¶ 4, 29.

⁴ *Id.* at ¶ 7.

⁵ *Id.* at ¶ 32.

challenged conduct of the defendant”; and (3) the injury would likely be redressed by a favorable judicial decision. *Spokeo, Inc. v. Robbins*, 578 U.S. 330, 338 (2016) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992)). It is the first prong that is the subject of Defendant’s motion to dismiss.

“To establish injury in fact, a plaintiff must show that he or she suffered ‘an invasion of a legally protected interest’ that is ‘concrete and particularized’ and ‘actual or imminent, not conjectural or hypothetical.’ ” *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560). To demonstrate imminence, allegations of future injury “suffice if the threatened injury is ‘certainly impending’ or there is a ‘substantial risk’ that the harm will occur.” *Susan B. Anthony List*, 573 U.S. at 158 (quoting *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 414 n.5 (2013)). For concreteness, the question is “whether the asserted harm has a ‘close relationship’ to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms.” *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2200 (2021). Additionally, where the claimed injury is exposure to a substantial risk of future harm, a plaintiff can meet concreteness by alleging it caused “currently felt concrete harms.” *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–56 (3d Cir. 2022).

In the context of data breach litigation, disclosure of personal information does not amount to injury-in-fact where there are no specific allegations that a plaintiff’s personal information has been used in a way that caused harm or that such use is certainly impending. *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). “An increased risk of identity theft resulting from a security breach [is] [] insufficient to secure standing.” *Id.* at 43. The *Reilly* plaintiffs were employees of a law firm that had contracted with Ceridian to provide payroll services. A hacker infiltrated defendant’s computer systems, gaining access to the personal and

financial information of thousands of employees, *including names, social security numbers, birth dates, and bank account numbers*. *Id.* at 40. The plaintiffs alleged that the security breach increased the risk that their personal information would be misused or that they would be the subject of identity theft. *Id.* at 40. The Court held that the plaintiffs' allegations were insufficient to establish injury in fact because “[a]llegations of ‘possible future injury’ are not sufficient to satisfy Article III.” *Id.* at 42.

As was the case in *Reilly*, Plaintiffs’ contentions here rely “on speculation that the hacker: (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [plaintiffs'] names.” *Reilly*, 664 F.3d at 42. Plaintiffs’ “allegations of hypothetical, future injury are insufficient to establish standing” because Plaintiff’s will not sustain injury “[u]nless and until these conjectures come true.” *Id.*

In contrast to *Reilly*, the Third Circuit’s decision in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146 (3d Cir. 2022) found that a plaintiff in a data breach case did successfully allege an injury. The plaintiff in *Clemens*, was a former employee of ExecuPharm whose sensitive personal data—including her address, social security number, banking and financial account numbers, insurance and tax information, passport, and information related to her husband and child—was stolen during a ransomware attack. A known hacking group called “CLOP” accessed the employer’s servers and stole plaintiff’s personal data, held it for ransom, and later published it for sale on the Dark Web. The employer notified its employees of the breach and encouraged them to take precautionary measures. Plaintiff immediately conducted a review of her financial records and credit reports for unauthorized activity, placed fraud alerts on her credit reports,

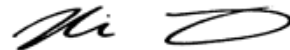
transferred her account to a different bank, enrolled in complimentary credit-monitoring services offered by defendant, and purchased additional credit monitoring services for herself and her family.

Concluding that the *Clemens* plaintiff alleged sufficient risk of future injury, the Court reasoned: “[b]ecause we can reasonably assume that many of those who visit the Dark Web, and especially those who seek out and access CLOP's posts, do so with nefarious intent, it follows that Clemens faces a substantial risk of identity theft or fraud *by virtue of her personal information being made available on underground websites.*” *Id.* at 157 (emphasis added). The Court further explained: “this set of facts clearly presents a more imminent injury than the ones we deemed to establish only a hypothetical injury in *Reilly.*” Although *Clemons* makes clear that “misuse [of the stolen data] is not *necessarily* required,” the fact that CLOP's actual publication of the plaintiff's information on the Dark Web was a deciding factor in distinguishing the alleged injury from *Reilly.* *See also Rauhala v. Greater New York Mut. Ins., Inc.*, No. CV 22-1788, 2022 WL 16553382, at *2 (E.D. Pa. Oct. 31, 2022) (denying Plaintiff's motion to remand where plaintiff class members' PII and PHI data was “accessed, stolen, and sold on the Dark Web”).

The present case is more factually analogous to *Reilly* than *Clemens*. As was the case in *Reilly*, this data breach involves an “*unknown* hacker who *potentially* gained access to sensitive information.” *Clemens*, 48 F. 4th at 156 (emphasis in original); *Reilly*, 664 F. 3d at 40. Plaintiffs do not allege that their PII and PHI data has been published or misused in any fashion. The forensic investigation performed by Defendants merely revealed that an unauthorized person *may* have accessed a data set including Plaintiff's personal information. Plaintiff's complaint relies on mere speculation about what *might* happen in the future. Moreover, unlike here, the personal information involved in *Clemens* was far more extensive. In addition to dates of birth,

full names, home addresses, and social security numbers, the hackers in *Clemens* gained access to and published taxpayer identification numbers, banking information, credit card numbers, driver's license numbers, sensitive tax forms, and passport numbers. While the additional harms outlined by Plaintiff, namely her emotional distress and time and money involved in mitigating the effects of the data breach, could be construed as *concrete* under *Clemons*, the injury still cannot be said to be *imminent* in the absence of any allegation that the information has been used in any manner. In conclusion, Plaintiff's allegations of hypothetical and future harm are too attenuated to establish Article III standing. An appropriate order to follow.

BY THE COURT:

A handwritten signature in black ink, appearing to read 'Mi D', is positioned above a horizontal line.

Hon. Mia R. Perez